PRIVACY IMPACT ASSESSMENT

Passport Information Electronic Records System (PIERS) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Passport Information Electronic Records System (PIERS)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: PIERS

(d) iMatrix Asset ID Number: # 85

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The system is currently undergoing the Assessment and Authorization process with an expected Authorization to Operate (ATO) by winter 2020.

(c) Describe the purpose of the system:

PIERS is a web-based application which manages passport records including Consular Reports of Birth Abroad (CRBAs), Certificates of Witness to Marriage (CWM), Consular Reports of Death Abroad (CRODA), Advance Finder (AF) and Diplomatic and Official Tracking System (DOTS) records, and Panama Canal Zone (PCZ) records data. PIERS provides structured query capabilities to the data maintained within its environment. It operates on the Department of State's (DoS) internal network and provides direct access for DoS users.

The PIERS system provides users with both case-based and user-based views of information and support for electronic checking and reporting of work processes. Case-based views refer to the different types of data records that the PIERS system and database maintain. This includes U.S. passport information (all records of issued and expired U.S. passports, not issued applications, and destroyed/ stolen/ lost U.S. passports) and consular records of overseas births and deaths. User-based views using the PIERS capabilities provide access to different data elements, record types, and system functions based on specific groups or system application roles assigned to individual users.

The main purpose of the PIERS application is to provide mission-critical support for timely and accurate processing of data requests for Passport Systems major applications. PIERS performs the following:

- Accepts the request from DoS user
- Places the request in the appropriate format for each database
- Collects a response from each of the various databases
- Builds a view of the response
- Sends a reply to the requester

The queries to the databases are processed in parallel, not in sequence, so that if a particular database is not operating, the overall process is not delayed.

PIERS information is shared externally with the Department of Homeland Security (DHS) and the U.S. Census Bureau (Census).

d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Name
- Date of birth
- Place of birth
- Country of birth
- Sex
- Social Security Number
- Phone number(s) (personal and work)
- Addresses (personal and work)
- Passport number, type, issuance date and expiration date
- Medical information
- Driver’s license or other identifying number(s)
- Education information
- Employment information
- Financial information
- Personal email addresses
- Biometric records
- Alias information
- Federal tax information

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2705 (Passports and Consular Reports of Birth Abroad)
- 22 U.S.C 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 C.F.R. Subchapter F (Nationality and Passports)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008; Executive Order 13880, July 11, 2019
- Title 13 of the U.S. Code (Census)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number:
  STATE-26 - Passport Records, March 24, 2015
  STATE-05 - Overseas Citizens Records and Other Overseas Records, September 8, 2016

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
Schedule number, Length of time the information is retained in the system, and Type of information retained in the system:

A-13-001a, b, c &d: Passport Records: Passport and Citizenship Case Files
Description: Case files containing passport applications, Consular Reports of Birth Abroad of U.S. Citizens; Certificates of Witness to Marriage, Applications for Amendment or Extension of Passport; Certificates of Loss of Nationality, and other supporting forms, documents and correspondence pertaining to each case.
Disposition: Transfer/destroy records in accordance with respective disposition authority cited below.
DispAuthNo: NC1-059-79-12, N1-059-04-02, N1-059-96-05, respectively

A-13-001-02 Passport Books: Recovered, Surrendered, Unclaimed or Found
Description: These passports books were issued to individuals who have returned them on their own initiative or at the request of the Department of State or other U.S. Government agency or have been found, recovered, and/or forwarded to Passport Services, Office of Technical Operations, Records Services Division (PPT/TO/S/RS). They include diplomatic or other official passports issued to military personnel who are either discharged, retired or deceased during the validity period of the passport; No Fee passports issued to Peace Corps volunteers; tourist passports; and all other passports.
Disposition: Destroy after receipt has been logged into PIERS database or successor electronic database. (ref. N1-059-96-5, item 2)
DispAuthNo: N1-059-04-2, item 2

A-13-001-16 Passport Lookout Master
Description: This on line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
DispAuthNo: N1-059-04-2, item 16

A-13-002-02 Requests for Passports
Description: Copies of documents relating to selected passport requests.
Disposition: Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 2

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 3

A-15-001-02 American Citizens Services (ACS) system
Description: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S.

citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts. ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes biographic information, case information, and case activity log.
Disposition: TEMPORARY. Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later.
NOTE: ACS case records are replicated to the Consular Consolidated Database each day for long-term recordkeeping.
DispAuthNo: N1-059-09-40, item 1

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?
26 U.S.C. 6039E (Information Concerning Resident Status) and
22 U.S.C. § 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008; Executive Order 13880, July 11, 2019

(c) How is the information collected?

No information is entered into PIERS by applicants. PIERS data and information is captured from other CA systems, i.e., Travel Document Issuance System (TDIS); Passport Record Imaging System Management (PRISM); American Citizen Services (ACS); Front End Processor (FEP); Management Information System (MIS) and the Consular Consolidated Database (CCD) and exported to PIERS directly.

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

Various quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

The accuracy of the information is checked against sources including, but not limited to, other CA systems which interface with law enforcement systems and systems at the Social Security Administration (SSA), Internal Revenue Service (IRS), and the Department of Homeland Security (DHS).

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Data processed by PIERS are retrieved from the Consular Affairs systems listed in paragraph 4(c) above. PIERS is dependent upon the validity and accuracy of data in these systems. Ensuring the information is current is the responsibility of the individual completing the application for services via the CA systems. Applicants can modify or amend records by accessing the website where the record was established in the source CA system. Individuals who wish to have their records amended in the source site where services were requested can find instructions, submission requirements, and the address of the pertinent offices in the System of Records Notices (SORN), STATE-26 and STATE-05, posted on the DoS Privacy Office website. Information can also be updated during the adjudication process for services requested.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not acquire information from commercial sources nor is it publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

N/A. PIERS does not collect information from the public.

However, the applicant is advised of all the relevant privacy implications via a Privacy Act Statement at the time the individual completes and signs the application at the source of collecting the information via paper form or electronic system.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

N/A. PIERS does not collect information directly from the public. PIERS receives information from the CA systems listed in paragraph 4(c).

(j) How did privacy concerns influence the determination of what information would be collected by the system?

PIERS does not collect information from the public. PIERS receives information from other CA systems addressed in paragraph 4(c).

The Department of State understands the need for PII to be protected. The PII in PIERS is handled in accordance with federal privacy regulations and is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. The collection of PII is limited to only what is required for the systems to perform the functions for which it is intended, providing structured query capabilities to the data maintained within PIERS for the management and processing of U.S. passports.

5. Use of information

(a) What is/are the intended use(s) for the information?

The PII in PIERS is used to manage and process U.S. passport requests and applications for other consular products. Case-based views of information are used to manage and track record access cases for issued U.S. passports, providing information such as reasons for adjudication decisions for use in processing U.S passports. Such information includes all records of issued and expired U.S. passports, not issued applications, destroyed/stolen/lost U.S. passports and consular records of overseas births and deaths.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information assists in the operations and management of the passport application process. The information also assists the Census Bureau in collecting information about citizenship status in connection with the decennial census in accordance with Executive Order 13880, July 11, 2019.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internal DoS Sharing:

The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the PIERS system will be shared internally with other CA systems PRISM, ACS, FEP and CCD.

Internal sharing of information outside of CA/CST also includes sharing with the Bureau of Diplomatic Security (DS).

External DoS Sharing:

PIERS information is indirectly shared with DHS via the Consular Consolidated Database (CCD). CCD pulls passport reports and data from PIERS and electronically transmits to the DHS.

PIERS will share an extract of digitized U.S. passport records from January 1, 1978, to July 31, 2020, with the U.S. Census Bureau for the decennial census.

(b) What information will be shared?

Internal: The PII information in paragraph 3d is shared with the CA Systems PRISM, ACS, FEP and CCD.

External: The PII identified in paragraph 3d (with the exception of Federal Tax information that is used internally within CA/CST to process passports) is shared with DS and DHS. The extract of the PIERS PII data shared with the U.S. Bureau of Census includes the applicant's full name, social security numbers, aliases, passport number, passport type, passport issuance and expiration dates, date and place of birth, sex, and mailing address.

(c) What is the purpose for sharing the information?

Internal: The information shared with the Bureau of Diplomatic Services is to assist the Department of State in facilitating investigations of fraud and other criminal acts that fall under DS jurisdiction, to include fraud identified during the passport application process.

PIERS information shared with CA Systems PRISM, ACS, FEP, and CCD is used to manage and process U.S. passport requests and applications.

External: PIERS passport information shared via the CCD system with DHS is to validate applicant information and to preclude fraudulent activity.

Information shared with the U.S. Census Bureau will be used to assist in improved estimates of population characteristics related to citizenship and to improve data collection and record linkage methods for surveys and censuses conducted under Title 13 of the U.S. Code.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal: All information is shared using Department of State approved secure Information System Connection Ports, Protocols and Services. All of the CA systems reside on the Department's secure internal network, OpenNet.

Internal CA/CST information is shared by direct secured communications (database to database) using transport and message level security interfaces with other State Department systems. Information is shared with DS via phone, email etc.

External: Information is shared electronically with DHS through the Consular Consolidated Database by utilizing secure transport layer security methods.

Information shared with the U.S. Census Bureau is transmitted via Census provided managed file transfer (MFT) system which utilizes inflight encryption transport layer security in addition to advanced encryption. DoS will additionally compress the data files in a password-protected zip file prior to transmission.

Both methods to transmit information to DHS and the U. S. Census Bureau are permitted under Department of State policy for handling and transmission of sensitive but unclassified information.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: Supervisors along with the site Information System Security Officers (ISSOs) determine individualized access levels depending on job function and level of clearance. PIERS users must comply with U.S. government requirements for the protection and use of PII.

Information is shared by secure transmission methods permitted by internal State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the State Department domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access. Defense in depth is deployed as well as roles assigned based on least privilege. Finally, regularly administered security and privacy training informs authorized users of proper handling and safeguard procedures.

External: PIERS Information shared with DHS is via the Consular Consolidated Database, utilizing secure transport layer security methods. A Memorandum of Understanding in addition to an Inter-connection Sharing Agreement is in place with DHS safeguarding the handling and transmission of information.

Information shared with the Census Bureau will be transmitted via a managed file transfer (MFT) system which utilizes inflight encryption transport layer security in addition to advanced encryption. An Information Sharing Agreement and Memorandum of Understanding is in place with the U.S. Census Bureau outlining the safeguards in place for the use and handling of the passport information provided by the DoS.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:

   Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

2) Strict role based access control, based on approved roles and responsibilities, authorization, need-to-know, and clearance level.

3) Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

‘

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

PIERS does not collect information from individuals. Individuals must follow processes of the source systems used to apply for the specific service to request correction of their information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can follow procedures outlined in the Passport Records SORN, STATE-26 and Overseas Citizens Records and Other Overseas Records SORN, STATE-05 posted on the

Department of State's Privacy website for the source site where individuals applied for the specific services.

(c) By what means are individuals notified of the procedures to correct their information?

This is not applicable; PIERS does not collect information from individuals, however, notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals who wish to have their records amended in the source site where services were requested can find instructions, submission requirements, and the address of the U.S. Department of State, Passport Services, Office of Legal Affairs, Law Enforcement Liaison Division (CA/PPT/S/L/LE) in SORNs STATE-26 and STATE-05, posted on the Department of State's Privacy website, www.state.gov/privacy.

8. Security Controls

(a) How is the information in the system secured?

PIERS is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized State Department users, including cleared contractors who have a justified need for the information in order to perform official duties.

All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

CA Systems are configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and are tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the system, individuals must be authorized users of the Department of State's unclassified internal network which requires a background investigation and an application approved by the supervisor and the site ISSO. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data is recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. If an issue were to arise, administrators of the system would review or (audit) the logs that were collected from the time a user logged on until the time he/she logs off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory Cyber Security Awareness training (PS800) is required for all users of State Department systems. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. State Department personnel are also required to take the biennial privacy course, Protecting Personally Identifiable Information (PA318). In addition to the above required training, the Passport Services Internal Control Guide requires all personnel (government and contractors) to complete the Passport Data Security Awareness (PC441) course and pass the course as an annual recertification to maintain PIERS access. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.

The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they acknowledge and agree to the rules and to protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

☒Yes ☐No

If yes, please explain.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Resource Management Office Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. All systems must comply with all guidelines published by Information Resource Management Office Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

PIERS uses Transmission Control Protocol/Internet Protocol TCP/IP to assist with its data transport across the network. Data in transit is encrypted. The TCP/IP suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary.

(f) How were the security measures above influenced by the type of information collected?

The information collected contains PII of U.S. Citizens and Legal Permanent Residents (LPRs). Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

The following personnel have access to these systems:

PIERS OpenNet Users - Department of State employees and contractors working domestically and overseas in connection with processing passports.

System Administrators - System Administrators have access to PIERS. They manage the computer system, including its operating system and the various supporting applications.

Database Administrators - Database Administrators are authorized to access the database for the purpose of performing maintenance, troubleshooting technical issues, software upgrades; patch/hot fix application, backups and configuration to the database.

(b) How is access to data in the system determined?

An individual's job function determines what data can be accessed as approved by the supervisor and the site Information Systems Security Officer (ISSO). Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in PIERS.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

There are three types of PIERS user roles: PIERS OpenNet Users (Department of State employees and contractors), System Administrators, and Database Administrators. Separation of duties and least privilege are employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

PIERS Users- Access to PIERS is restricted to cleared Department of State direct hire and contractor employees. DoS employees and contractors receive their access by requesting access from the CA organization in compliance with 12 FAM policies. Each user must submit a DoS internet (OpenNet) Account Request Form indicating the system he/she needs access to in order to do his/her job. The account request is reviewed by the user's supervisor and must be approved by the system manager before the request can be granted. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

System Administrator - The System Service and Operations Project Manager completes the CA Consular Systems and Technology System Administrator Account Request Form. The Project Manager reviews the role and approves the form authorizing the account to be established and activated, and a current System Administrator creates the account. System administrators have logon identifications associated with their name that allows for user auditing.

Database Administrators - DBA access is controlled by the Integrated Services (IS) team through the use of access control lists (ACLs) as established by the system administrators. PIERS DBAs are authenticated using Windows operating system authentication. The CA ISSO is responsible for reviewing and approving DBA accounts.

Access to PIERS is restricted to cleared Department of State direct hire and contractor employees who have been granted access rights and privileges to perform specific jobs.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

PIERS information is protected by multiple layers of security controls including:

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role based as required by policy.

- PIERS System & Database Administrators and internal users have access via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing PIV/CAC and PIN to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to the person who performed the activity.

- Least Privileges are restrictive rights/privileges or accesses of users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.